

## Practice on PA and Computability

### The power of induction

Recall the axioms of PA:

- **P1**  $Sx \neq 0$
- **P2**  $Sx = Sy \rightarrow x = y$
- **P3**  $x + 0 = x$
- **P4**  $x + Sy = S(x + y)$
- **P5**  $x \cdot 0 = 0$
- **P6**  $x \cdot Sy = x \cdot y + x$
- **Ind <sub>$\varphi$</sub>**   $\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(Sx)) \rightarrow \forall x \varphi(x)$

#### Exercise 0.1.

Show that  $\text{PA} \vdash \forall x(Sx \neq x)$

But we need induction to prove this, even if we throw in another axiom:

- **P7**  $\forall x (x \neq 0 \rightarrow \exists y(x = Sy))$

The system (P1)-(P7) is referred to as **Robinson's Q**

#### Exercise 0.2.

Show that  $Q \not\vdash \forall x(Sx \neq x)$

(Construct a model of **Q** by adding a “point at infinity” to  $\mathbb{N}$  and defining the operations  $S, +$  accordingly.)

If we use induction in the *metatheory* (i.e. the theory we are using to reason about **Q**, **PA**, etc.), we can still show

$$\text{for all } n \in \mathbb{N}, \quad Q \vdash S\underline{n} \neq \underline{n}$$

## Capturing basic arithmetic of $\mathbb{N}$ in $\text{PA}^-$

We saw in class that  $\text{PA}^-$  proves all true  $\Sigma_1$ -statements about  $\mathbb{N}$ . This is due to two facts:

- $\Delta_0$ -formulas are **absolute between structures and end-extensions thereof**.
- Any model  $\mathcal{M}$  of  $\text{PA}^-$  is an end-extension of (an isomorphic copy of)  $\mathbb{N}$ .

To prove the second fact, we need to show two things:

1. The mapping  $\iota : n \mapsto \underline{n}^{\mathcal{M}}$  is an embedding (so  $\iota(\mathbb{N})$  is a substructure of  $\mathcal{M}$  isomorphic to  $\mathbb{N}$ ).
2. Any element  $y \in M$  with  $y <^{\mathcal{M}} \underline{n}^{\mathcal{M}}$  is itself some  $\underline{m}^{\mathcal{M}}$ .

The first item is established in the next exercise.

#### Exercise 0.3.

Show that for all natural numbers  $n, k, l$ ,

$$\begin{aligned} n = k + l &\implies \text{PA}^- \vdash \underline{n} = \underline{k} + \underline{l} \\ n = k \cdot l &\implies \text{PA}^- \vdash \underline{n} = \underline{k} \cdot \underline{l} \\ n < k &\implies \text{PA}^- \vdash \underline{n} < \underline{k} \end{aligned}$$

(You prove this by induction in the metatheory. For example, for the first statement, the case  $k = 0$  follows from axiom (A6). For the inductive step, use axiom (A1).)

For the second item:

**Exercise 0.4.**

Show that for all  $k \in \mathbb{N}$ ,

$$\text{PA}^- \vdash \forall x (x \leq \underline{k} \rightarrow (x = \underline{0} \vee \dots \vee x = \underline{k}))$$

Again, use (meta-) induction on  $k$ . The case  $k = 0$  follows from (A15). For the inductive step, show

$$\text{PA}^- \vdash \forall x, y (y > x \rightarrow y \geq x + 1)$$

**More on the limitations of  $\text{PA}^-$**

**Exercise 0.5.**

Let  $R$  be the ring  $\mathbb{Z}[X, Y]/(X^2 - 2Y^2)$ , i.e.,  $R$  is the polynomial ring  $\mathbb{Z}[X, Y]$  modulo the equivalence

$$p(X, Y) \sim q(X, Y) \quad : \iff \quad p - q = r(X^2 - 2Y^2).$$

Show that  $R$  can be discretely ordered.

Infer that

$$\text{PA}^- \not\vdash \forall x, y (x > 1 \rightarrow x^2 \neq 2y^2)$$

(Is this fact provable in  $\text{PA}$ ?)

**Number theoretic functions**

**Exercise 0.6.**

Show that the following relations and functions are primitive recursive.

$x$  divides  $y$   
 $\text{rem}(x, y)$  (remainder when  $y$  is divided by  $x$ )  
 $x$  is prime  
 $n \mapsto p_n$ , where  $p_n$  is the  $n$ th prime

**Gödel's Lemma**

If you feel like it, try your hands at proving Gödel's famous Lemma on the  $\beta$  function:

**Lemma 0.1** (Gödel's Lemma).

There exists a primitive recursive function  $\beta$  such that for every  $k$  and for every finite sequence  $x_0, x_1, \dots, x_{k-1} \in \mathbb{N}$ , there exists a natural number  $c$  with

$$\text{for all } i < k : \beta(c, i) = x_i.$$

In fact, there exists a  $\Delta_0$ -formula  $\theta(x, y, z)$  such that

$$\mathbb{N} \models \forall x, y \exists! z \theta(x, y, z),$$

and the formula  $\theta(x, y, z)$  defines the function  $\beta$  over the natural numbers.

*Hint:* To code a sequence  $x_0, x_1, \dots, x_{k-1}$  of natural numbers, set  $m = b!$  where  $b = \max(k, x_0, x_1, \dots, x_{k-1})$ . Verify the numbers

$$m + 1, 2m + 1, \dots, k \cdot m + 1$$

are pairwise coprime. Now try to apply the *Chinese Remainder Theorem*.